from an application server indicating an authorization to communicate with the application server, the application server interface further configured to monitor the session between an application server and a browser; and

a load balancing device configured to receive browser requests among a plurality of webservers, wherein the load balancing device is further configured to screen the browser requests according to predetermined criteria including preauthorization indicia, wherein browser requests are prevented from making an unfriendly attack to the system.

2. (Amended) A system according to Claim 1, wherein the application server interface is configured to communicate with an application server only when a signal is received by the webserver that authorizes such communication according to privileges associated with a browser prevent an unauthorized attack from multiple browser requests that may shut down an application server if the browser requests were allowed direct access.

3. (Amended) A system according to Claim 2, wherein the application server interface includes a monitoring mechanism for monitoring the activity of the application server during a session with a browser and a screening mechanism configured to prevent access to browser requests that are not authorized to access an application server according to predetermined privileges.

4. (Amended) A system according to Claim 2, wherein the application server interface includes a monitoring thread from for facilitating the monitoring by the webserver of the activity of the application server during a session with a browser, the state server configured to define privileges associated with a browser request that define the parameters in which a browser may access an application server.

5. (Amended) A system according to Claim 2, wherein the application server interface is further configured to receive a monitoring thread from an application server so that the webserver can monitor the activities of a application server during a session between the application server and a browser, the state server configured to define privileges associated with

a browser request that define the parameters in which a browser may access an application server including limits to predefined information or services.

6. (Amended) A system according to Claim 2, wherein the application server interface is further configured with a monitoring mechanism that allows an application server to monitor the activities of a webserver during a session between the application server and a browser, the state server configured to define privileges associated with a browser request that define the parameters in which a browser may access an application server including predetermined commands a browser may send to the application server indicative of an unauthorized attack by multiple browser commands.

7. (Amended) A system according to Claim 2, wherein the application server interface is further configured to receive a monitoring thread from an application server so that an application server can monitor the activities of a webserver during a session between the application server and a browser, the state server configured to define privileges associated with a browser request that define predetermined commands a browser may send to the application server indicative of an unauthorized attack by multiple browser commands.

8. (Amended) A system according to Claim 2, further comprising a second webserver communicating with the other webserver and with the state server, wherein the second webserver is further configured to take over a session occurring between the application server and a browser being monitored by the other webserver in the event the other webserver stops monitoring the session that is associated with a browser request that has been screened and authorized to access an application server.

Cancel Claims 9 and 10

11. (Amended) A system for communicating among a plurality of network servers communicating with a plurality of computers and for preventing unauthorized attacks of browser attacks directed to an application server, comprising:

a plurality of webservers communicating with and configured to receive a request from a web browser and to screen and route the browser request to an application server upon the receipt of a signal from the application server, wherein each webserver is configured to maintain

information related to the authorization of browser requests to prevent multiple unauthorized browser attacks directed to an application server;

an application server interface configured to control communication between the plurality of webservers and an application server;

a state server configured to store data related to communication sessions occurring among a web browser, a webserver and an application server, wherein a first webserver is configured to retrieve information related to a session between a web browser and an application server and being monitored by a second webserver in the event that the second webserver terminates its monitoring of the session; and

a load balancing device configured to receive browser requests among a plurality of webservers, wherein the load balancing device is further configured to screen the browser requests according to predetermined criteria including preauthorization indicia, wherein browser requests are prevented from making an unfriendly attack to the system.

12. (Amended) A system according to Claim 11 further comprising a database communicating with the state server and configured to store session information and for storing and maintaining browser request privileges that define whether a browser is authorized to access an application server to prevent direct attacks of browser attacks on application severs.

13. (Amended) A system according to Claim 11, wherein the webserver is configured to route a browser request to an application server only upon the receipt of a signal from the application server indicating that the application server is ready to receive browser requests, and wherein the state server is configured for storing and maintaining browser request privileges that define whether a browser is authorized to access an application server to prevent direct attacks of browser attacks on application severs.

14. (Amended) A system according to Claim 11 further comprising a load balancing device configured to receive browser requests sent from computers communicating with the network system and to direct the requests among the plurality of [webservers] application servers, wherein the state server is configured for storing and maintaining browser

request privileges that define whether a browser is authorized to access an application server to prevent direct attacks of browser attacks on application severs.

15. (Amended) A method of facilitating communication between a web browser and an application server, comprising:

receiving a request for access to an application server;

receiving the request by a first webserver;

screening the request for determining authority to access the application server by accessing the state server to determine whether a browser is authorized to access an application server to prevent attacks by multiple browser requests;

receiving a signal from the application server indicating that it is ready to receive a browser request;

communicating with the application server to create a monitoring thread between the webserver and the application server; and

if the browser request is screened and authorized to access the application server, facilitating communication between the browser and the application server with the webserver.

16. (Amended) A method according to Claim 15, further comprising:

communicating with a state server to create a monitoring mechanism between the webserver and the state server to monitor communications between a web browser and an application server and to store information related to such communications and to store privilege information associated with browser requests and information related to multiple unauthorized browser requests to allow the system to prevent attacks by multiple browser requests.

17. (Amended) A method according to Claim 15, further comprising:

routing the incoming browser request to one of a plurality of webservers;

screening the browser requests by retrieving browser request privilege information from the state table and determining whether the browser request is authorized to be sent to an application server to prevent unauthorized access to an application server with browser requests;

receiving the request by a first webserver; and

transferring identification information related to other webservers to the application server.

18. (Amended) A method according to Claim 15, wherein the step of facilitating communication between the application server and the webserver includes facilitating a session of communication between the application server and the webserver and to facilitate access only by authorized browser requests to prevent attack on an application server by browser requests.

19. (Amended) A method according to Claim 15, wherein facilitating communication between the browser and the application server with the webserver is done in response to receiving a signal from the application server indicating that it is ready to receive a browser request and in response to preauthorization of access of a browser request to an application server by a webserver by accessing the state table to determine the browser request privileges.

21. (Amended) A method according to Claim 15, wherein the step of facilitating communication between the application server and the webserver includes facilitating a session of communication between the application server and the webserver in response to receiving a signal from the application server indicating that it is ready to receive a browser request and in response to preauthorization of access of a browser request to an application server by a webserver by accessing the state table to determine the browser request privileges.

Cancel Claim 22